

WHAT IS CLAIMED IS:

1. A method for automatically controlling access from a remote client to a host server that has predefined access parameters, comprising:

determining an actual location of the remote client; and

5 using the actual location of the remote client to automatically control access to the host server based on the predefined access parameters.

2. The method of claim 1, further comprising controlling access to certain levels of data on the host sever based on the remote client's actual
10 location.

3. The method of claim 1, wherein the actual location of the remote client is determined by a global positioning satellite system.

4. The method of claim 1, further comprising using triangulation to determine the actual location of the remote client.
15

5. The method of claim 4, further comprising using three dimensional triangulation to provide latitudinal, longitudinal and elevational data to the remote client.
20

6. The method of claim 1, wherein the host server and the remote client operate in a networking environment.

7. The method of claim 1, wherein the networking environment is an extranet using a virtual private network with the Internet as the network communication channel.
25

8. The method of claim 1, wherein using the actual location of the remote client to automatically control access includes automatically preventing
30 unauthorized access of data on the host server based on locations where

access is not likely to occur by the remote client.

5 9. A tracking system for automatically controlling access from a remote client to a host server that has predefined access parameters, comprising:

a positioning device that determines an actual location of the remote client; and

10 a control module that uses the location of the remote client to automatically control access to the host server based on the predefined access parameters.

15 10. The tracking system of claim 9, wherein the control module controls access to certain operational interfaces of the host server based on its actual location.

20 11. The tracking system of claim 9, wherein the actual location of the remote client is determined by a global positioning satellite system.

25 12. The tracking system of claim 9, further comprising controlling access to certain predefined types of data on the host sever based on the remote client's actual location.

30 13. The tracking system of claim 9, wherein the control module automatically prevents unauthorized access of predefined data on the host server based on locations where access is not likely to occur by the remote client.

14. The tracking system of claim 9, wherein the positioning device receives data from a transmitter system that uses triangulation to determine the actual location of the remote client.

15. The tracking system of claim 14, wherein the transmitter system uses three dimensional triangulation to provide latitudinal, longitudinal and elevational data to the remote client.

5 16. The tracking system of claim 9, wherein the remote client is a personal computer connected to an extranet via the Internet and a virtual private network.

10 17. The tracking system of claim 9, wherein when plural remote clients attempt access to the host server from respective various locations, access to the host server by each remote client is automatically at least one of provided, denied or qualified, depending on the predefined access parameters and the location of each remote client at the time access is requested.

15 18. A computer-readable medium having computer-executable instructions for performing a process between a remote client and a host server having predefined access parameters, comprising:

20 determining an actual location of the remote client; and
using the actual location of the remote client to automatically control access to the host server based on the predefined access parameters.

25 19. The process of claim 18, wherein using the actual location of the remote client to automatically control access includes controlling access to certain predefined operational interfaces and types of predefined data on the host server based on its actual location.

30 20. The process of claim 18, further comprising, preventing unauthorized access to the host server by the remote client based on locations where access is not likely to occur by the remote client.